ELECTRONIC PRIVACY INFORMATION CENTER

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	**)**	
	)	
Rules and Regulations Implementing	**)**	**FCC Docket No. 04-53**
the Controlling Pornography and	**)**	
Marketing Act of 2003	**)**	

To: The Commission

COMMENTS OF
THE ELECTRONIC PRIVACY INFORMATION CENTER
April 30, 2004

Pursuant to the notice published by the Federal Communications Commission ("Commission") on March 31, 2004 regarding unwanted mobile service commercial messages and the CAN-SPAM Act, the Electronic Privacy Information Center submits the following comments.[1]

In passing the Telephone Consumer Protection Act of 1991 ("TCPA"), Congress shielded wireless devices from automatic dialer, prerecorded, and artificial voice telemarketing. The Commission should strive to enhance this shield, and prevent commercial messages to wireless devices from becoming the scourge that spam has become to individuals with e-mail accounts. The Commission's actions in this arena are extremely important, as more individuals are receiving SMS and e-mail on wireless phones. If the Commission fails to shield these devices from an onslaught of "mobile service commercial messages," ("MSCMs") consumers will not adopt these technologies, or use them to a more limited extent by keeping them powered off. Furthermore, since many users are charged for SMS or for bandwidth associated with receiving messages, it is unfair to allow commercial senders to transfer the costs of their advertising onto the user. Because of cost and annoyance risks, literally, the survival and utility of wireless communications devices depends on Commission action to provide isolation from constant commercial interruption.

I. The Commission Should Employ Its Authority to Regulate Autodialers to Prohibit Senders of Bulk or Automated Commercial Electronic Mail from Sending MSCMs

Under the TCPA, Congress empowered the Commission to regulate to use of "autodialers," devices that have the capacity to dial stored or randomly-produced telephone numbers.[2] In effect, spammers use modern autodialers to send SMS and e-mail over the Internet that is converted by the carrier to a SMS. Spammers either randomly generate e-mail addresses (which

[1] Rules and Regulations Implementing the Controlling Pornography and Marketing Act of 2003; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 69 Fed. Reg. 16873 (Mar. 31, 2004).
[2] 47 U.S.C. § 227 (b)(2), (a)(1).

in some cases are simply phone numbers followed by the domain name of a wireless provider, *i.e.* 202.555.1212@attws.net) or they use addresses stored by list brokers or harvesters for transmission to the wireless carrier. Accordingly, spammers store or produce large lists of contact information and use software to automate the initiation of the messages in bulk. For purposes of the TCPA, the Commission should view these activities as equivalent to employing an autodialer and prohibit the practice flatly with respect to transmission of both SMS and e-mail delivered to carriers that is converted to SMS.

The Commission should also address the issue of wireless devices that come with dedicated e-mail addresses. Typically, the user does not direct this e-mail address to a standard computer. Rather, the messages are delivered directly to the device. For instance, T-Mobile's Sidekick device is assigned an e-mail account under the tmail.com domain. That mail is not forwarded from another service to the device, rather, it is more akin to SMS service. The Commission should apply its autodialer rules to these e-mail addresses as well, as they are dedicated to wireless addresses, and act as a sort of enhanced SMS. Accordingly, the Commission should interpret these dedicated wireless-only domains as a conduit for messages transmitted directly to a wireless device used by a subscriber of a commercial mobile service.

II. The Commission Should Interpret Section 14(b)(1) to Prohibit All Senders of Commercial Electronic Mail from Sending MSCMs Unless the Sender Obtained Affirmative Consent

a. Wireless Telephones Are a Safe Haven from Telemarketing; They Should Also Be a Safe Haven from MSCMs

Wireless communications devices are considered highly personal by their users. Millions of individuals carry wireless devices everywhere they go. In part, the success of wireless devices and users' trust in them can be attributed to their status as a safe haven from telemarketing. Individuals trust that when their wireless phone rings, a friend or family member will be on the line, rather than a telemarketer. This trust in wireless service was created by Congressional action. In 1991, Congress passed the Telephone Consumer Protection Act, which created protections both for residential and wireless phone services.[3] Specifically, Congress flatly prohibited the use of autodialed, prerecorded voice, and artificial voice telemarketing to paging services, cellular telephone services, or any service for which the called party is charged for the call.[4] Other services found to deserve the same level of privacy protection included emergency "911" lines and hospital rooms.[5] As a result of Congress' action, generally, wireless telephones do not receive telemarketing calls.

In the sections below, we articulate why the Commission should continue to protect this safe haven from commercial messaging, and why the burden of proving the value of commercial wireless messages should fall upon businesses rather than consumers, who increasingly clamor for insulation from invasive marketing. We specifically urge the Commission to create an opt-in

[3] Public Law 102-243, 47 U.S.C. § 227.
[4] *Id*. at (b)(1).
[5] *Id*. at (b)(1)-(2).

standard for § 14(b)(1). The Commission should prohibit all senders of commercial electronic mail from sending MSCMs unless the sender obtained affirmative consent.

b. Affirmative Consent, or "Opt-In" Restrictions Are Consistent with Other Privacy Laws, and Have Been Found to Be Constitutional

An opt-in framework would better protect individuals' rights, and is consistent with most United States privacy laws. For instance, the Family Educational Rights and Privacy Act, Cable Communications Policy Act, Electronic Communications Privacy Act, the Video Privacy Protection Act, the Driver's Privacy Protection Act, and the Children's Online Privacy Protection Act all empower the individual by specifying that affirmative consent is needed before information is shared or used for secondary purposes, such as direct marketing.[6]

The courts have upheld opt-in approaches to in *Destination Ventures, Ltd. v. FCC*[7] and *Moser v. FCC*[8] and have continued to do so in recent years, especially where the cost of the communication is transferred onto the recipient.[9] In *Moser*, the Ninth Circuit upheld a section of the TCPA that banned automated telemarketing calls where the recipient had not expressly opted in to receive them. The Ninth Circuit found that automated telemarketing calls were a "threat to privacy," and that the statutory opt-in solution was narrowly tailored to advance the privacy interest.[10] *Destination Ventures*, also decided in the Ninth Circuit, affirmed TCPA provisions that prohibited sending unsolicited fax advertisements absent opt-in consent of the recipient. The statute defines "unsolicited advertisement" as any advertising "transmitted to any person without that person's prior express invitation or permission."[11] Thus, unless a recipient opts in, the fax is prohibited. The Ninth Circuit found that this regulation of commercial speech was not only permissible, but also desirable, as it was not overbroad in protecting the government's interest in preventing the waste of recipients' time and resources.

Nixon v. American Blast Fax cited *Destination Ventures* favorably and specifically addressed the unfeasibility of the opt-out approach.[12] The appellants in *Nixon*, Fax.com, argued that an opt-out scheme for the TCPA would be less restrictive, and that the TCPA was therefore too broad in its opt-in requirement. The court disagreed, and stated that "[w]hile it is true that the effect of TCPA will be that some consumers will not receive unsolicited advertisements they might have appreciated, under the approach advocated by Fax.com there would *always* be individuals suffering costs and interference from unwanted advertisements."[13]

---

[6] Respectively, at 20 U.S.C. § 1232 g, 47 U.S.C. § 551, 18 U.S.C. § 2510 et. seq., 18 U.S.C. § 2710, 18 U.S.C. § 2721, and 15 U.S.C. § 6501.
[7] 46 F.3d 54 (9th Cir. 1995).
[8] 46 F.3d 970 (9th Cir. 1995) *cert. denied*, 515 U.S. 1161 (1995).
[9] *See Missouri ex rel. Nixon v. American Blast Fax, Inc.*, 323 F.3d 649 (8th Cir. 2003) ("*Nixon*"). *See also Trans Union Corp. v. FTC*, 245 F.3d 809 (D.C. Cir. 2001), *petition for rehearing denied*, 267 F.3d 1138, *and cert. denied*, 536 U.S. 915 (2002); *Reno v. Condon*, 528 U.S. 141 (2000) (upholding opt-in requirements of the Driver's Privacy Protection Act); *but see U.S. West, Inc. v. Fed. Communications Comm'n*, 182 F.3d 1224 (10th Cir. 1999), *cert denied sub nom. Competition Policy Inst. v. U.S. West, Inc.*, 530 U.S. 1213 (2000).
[10] *Moser*, 46 F.3d at 975.
[11] *Id.* § 227(a)(4).
[12] *Nixon*, 323 F.3d at 656.
[13] *Id.* at 659 (emphasis added).

Trans Union upheld the Federal Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681 et seq. (2004), which, among other things, requires opt-in consent before consumer reporting agencies can use credit reports for marketing.[14] The court refused to consider opt-out because the data about consumers was not speech subject to strict First Amendment scrutiny.[15] On petition for rehearing, the court concluded that even under intermediate scrutiny, opt-in was narrowly tailored to advance the substantial government interest in protecting consumer privacy.[16]

Preventing the spread of MSCMs is similar to the bans placed on junk faxes in the TCPA. In both cases, the cost of the communication is transferred to the recipient. With regard to junk faxes, the cost comes from tying up the fax machine, wasted paper, and wasted ink. Similarly with regard to MSCMs, an opt-in approach will prevent wireless users from having their time wasted, from marketers filling up their small storage space with gratuitous marketing, from being charged for receiving SMS messages or messages that count against a bandwidth allotment, and from the constant interruption that spam causes to Internet users. An opt-in approach is consistent with existing law, and would be upheld if challenged in court.

c. Public Opinion Clearly Supports Opt-In Over Opt-Out

Public opinion clearly supports an opt-in system for information collection and sharing. A study conducted by the American Society of Newspaper Editors (ASNE) and the First Amendment Center (FAC) in April 2001 illustrated strong support for privacy and specifically for opt-in systems.[17] In that study, the respondents indicated that personal privacy was an issue as important as crime, access to health care, and the future of the Social Security system.

In information collection contexts, individuals regularly indicate that opt-in is preferable to opt-out. The ASNE/FAC study shows that 76% of individuals support opt-in as a standard for sharing of driver's license information. A study conducted by Forrester Research found that 90% of Internet users want the right to control how their personal information is used after it is collected.[18] A study conducted by the Pew Internet and American Life Project found that 86% of Internet users favor opt-in privacy policies.[19] And, a Businessweek/Harris poll in 2000 found that 86% favored opt-in over opt-out. The same poll showed that if given a choice, 90% of Internet users would either always or sometimes opt-out of information collection.[20]

---

[14] *Trans Union*, 245 F. 3d 809.
[15] *Id.* at 819. *See also Trans Union v. FTC* , 267 F.3d 1138, 1142 (2001) (holding that opt-in is narrowly tailored to meet interest in protecting personal financial data).
[16] *Trans Union v. FTC*, 267 F.3d at 1142.
[17] Anders Gyllenhall & Ken Paulson, *Freedom of Information in the Digital Age*, April 2001, at http://www.freedomforum.org/.
[18] *The Privacy Best Practice*, Forrester Research, Sept. 1999.
[19] Susannah Fox, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, the Pew Internet & American Life Project, Aug. 20, 2000.
[20] *Business Week/Harris Poll: A Growing Threat*, Businessweek, Mar. 20, 2000, at http://www.businessweek.com:/2000/00_12/b3673010.htm.

A study released this month by Yankelovich Partners highlighted individuals' growing frustration with invasive marketing.[21] In a "recontact survey" of 601 respondents from February 20-29, 2004, Yankelovich found that: 53% of consumers polled reported that spam had made them likely to ignore all marketing and advertising; 53% said that for the most part, marketing and advertising does not help them shop better; 59% feel that most marketing and advertising has very little relevance to them; 65% think there should be more limits and regulations on marketing and advertising; 69% are interested in products and services that would help them skip or block marketing; 33% would be willing to have a slightly lower standard of living to live in a society without marketing and advertising; 65% feel they are constantly bombarded with too much marketing and advertising ; 61% feel that the amount of marketing and advertising is out of control; and 60% have a much more negative opinion of marketing and advertising now than a few years ago.

The Yankelovich study shows that a clear majority of Americans want more insulation from irrelevant interruption. Choosing an opt-out framework, one where the burden falls upon the consumer to object to MSCMs, will create another enormous avenue for spam and constant interruption in our lives.

d. Opt-Out Is Inefficient Because It Shifts Burdens to Protect Privacy onto Millions of Individuals

An opt-out approach for MSCMs will not adequately protect individuals' interest in privacy because opt-out systems systematically fail to give consumers control over their personal information.[22] Opt-out approaches place an unreasonable burden on customers to remain constantly alert of a carrier's practices, and, if needed, take additional steps to protect their information from being freely distributed. In the context of MSCMs, opt-out is particularly inappropriate because many users pay for each SMS or for bandwidth associated with receiving e-mail on wireless devices. It is unfair to transfer these costs for unwanted messages onto the recipient.

In addition, there is substantial evidence concluding that opt-in is not only the more effective, but also the more desired way to protect customer information. Research shows that the opt-in method gives consumers meaningful choice, control over personal information, and automatic protection from privacy invasions where opt-out does not.[23] Additional studies reveal "the majority of the general public is still unaware of the exact nature of marketing uses and the availability of opt-out choices."[24] Moreover, the American public believes that opt-in is more likely to protect privacy.[25]

---

[21] YANKELOVICH MONITOR, Apr. 2004 (*Consumer Resistance to Marketing Reaches All-Time High*, Yankelovich Press Release, Apr. 15, 2004).

[22] *See* Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection* 329-30 (1996) ("The industry itself recommends the use of only vague notices that do not offer meaningful disclosure of practices.").

[23] Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self- Regulation is Inadequate*, 49 S.C. L. Rev. 847 (1998).

[24] *Id*. *See also* Privacy Rights Clearinghouse Second Annual Report 21 (1995), cited in Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1253 n.255 (1998) ("Many consumers are unaware of

We further note that at the time of this filing, nearly 60 million phone numbers have been enrolled into the telemarketing Do-Not-Call Registry. From the perspective of individuals, it would have been more efficient to simply create an opt-in system instead of requiring tens of millions of people to opt-out. With enrollment at that level, the Commission should assume that individuals generally do not want marketing on their telecommunications devices, and should have to shift the burden to marketers to obtain opt-in consent.

e. Congress Intended Heightened Protection for MSCMs Than Normal Spam

The Commission improperly interprets Congress' intent by stating that it believes "that in order to do so [avoid MSCMs], the consumer must take affirmative action to bar the MSCMs in the first place." The CAN-SPAM Act directs the Commission to "protect consumers from unwanted mobile service commercial messages."[26] It further states that the regulation should provide subscribers with the ability to "avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization."[27] This can be interpreted as direction to create an opt-in requirement that prohibits the transmission of the messages unless the sender had previously obtained affirmative consent. Since Congress created opt-out rights for recipients of normal spam, it makes sense to for the Commission to create opt-in rights for MSCMs in order to provide the greater protections intended by Congress.

III. "Express Prior Authorization" Should Be in Writing

Unless senders obtain express prior authorization from recipients in writing, recipients will face an extremely difficult hurdle in enforcing these regulations. It has been our experience from communication with junk fax litigants that junk fax broadcasters frequently claim that the recipient opted in to the transmission. At that point, the individual is forced to prove a negative—that consent had not been given at any time in the past. This is often an impossible challenge for litigants. Any number of thousands of transactions could have included language creating an existing business relationship or some consent to receiving the messages. A previous holder of the telephone number could have consented. Or the individual's family members may have consented. The Commission should not place individuals in the same situation when attempting to enforce their rights against senders of MSCMs. Affirmative consent should require a writing. That will shield legitimate senders from frivolous litigation and will assist individuals

---

personal information collection and marketing practices. They are misinformed about the scope of existing privacy law, and generally believe there are far more safeguards than actually exist.").

[25] *See* Testimony of Lee Rainie before the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce (May 8, 2001) (86 percent of Internet users surveyed stated that Internet companies should ask people for permission [opt-in] to use their personal information); EPIC's Polling Data Page, http://www.epic.org/privacy/survey/default.html; New York Senate Majority Task Force on the Invasion of Privacy, *Public Attitudes about the Privacy of Information*, at http://www.privacyrights.org/ar/invasion.htm at 11-12; Beth Givens, *What's Missing from this Picture? Privacy Protection in the New Millennium*, at http://www.privacyrights.org/ar/naag-mill.htm; and Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interests in the 21st Century*, at http://www.ag.state.mn.us/consumer/Privacy?Default.htm, at 20; Susannah Fox, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, The Pew Internet & American Life Project, Aug. 20, 2000, at 1.

[26] P.L. 108-187, at § 14(b).

[27] *Id*. at § 14(b)(1).

when their rights have been violated. It will also add a "ceremonial" nature to consent, where individuals are more likely to pay attention to the rights they are transferring to potential senders of MSCMs.

IV. If the Commission Chooses to Create A Registry, It Should Be Implemented at the Domain Level Rather than a Registry of Individual Subscriber Addresses.

If the Commission chooses to create a registry to assist individuals in avoiding MSCMs, it should implement it at the domain level rather than create a registry of individual e-mail addresses. Any such registry must protect individual privacy by collecting and disclosing only domain names of users that do not wish to receive emails.

A registry that collects and discloses individual email addresses frustrates several other spam reduction policies, including consumer approaches promulgated by the Federal Trade Commission.[28] The FTC has long recommended that consumers on the Internet protect their email addresses from disclosure to others as a way to reduce spam and prevent potential for fraud and identity theft. This guidance to consumers is designed to protect individual privacy and prevent abuse of email addresses from risks of fraud and identity theft (*e.g.*, "phishing").[29]

An email address-based registry would frustrate and hamper individual privacy interests and the FTC's anti-spam recommendations of non-disclosure of private email addresses. Disclosing individual email addresses to the list would allow spammers to find valid individual email addresses: the FTC has found evidence of email addresses harvesting for spam from email service directories.[30]

As a further example of how an email address-based registry could frustrate other anti-spam policy, a registry based on individual addresses unfairly places additional burden on users that change email addresses frequently to avoid spam. The FTC has advised consumers to set up such "disposable" addresses as one way to avoid spam.[31] With an email address-based registry, a consumer following the FTC advice would be burdened by having to reregister the new email address in the registry every time an email address change was made. By unfairly placing an additional burden on consumers, the individual email address registry would frustrate other anti-spam polices.

---

[28] FTC, Don't Want Your Email Address Harvested? (November 2002) *at* http://www.ftc.gov/bcp/conline/pubs/online/dontharvest.htm; FTC, "Email Address Harvesting: How Spammers Reap What They Sow (November 2002) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm; FTC, Consumer Alert: What's In Your Inbox? (April 2002) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/inbxalrt.htm; FTC, You've Got Spam: How to 'Can' Unwanted Email (April 2002) *at* http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm

[29] FTC, Is Someone 'Phishing' For Your Information (March 2004) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishregsalrt.htm; FTC, How Not to Get Hooked by a 'Phishing' Scam (July 2003) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm;

[30] FTC, Email Address Harvesting: How Spammers Reap What They Sow (November 2002) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm.

[31] FTC, Email Address Harvesting: How Spammers Reap What They Sow (November 2002) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm.

V. There Should Be No Exemption for Providers of Commercial Mobile Services

Polling in the area of privacy shows that people want less, not more, spam.[32] It makes little difference if the sender is a legitimate company, an illegitimate company, or even a company with which individuals regularly transact.

If the Commission chooses to create an exemption for commercial mobile services providers, the burden will be upon individuals to opt out. Again, opt-in is a more efficient solution for individuals, because telephone carriers have so poorly implemented opt-out mechanisms that it appears as though they are attempting to frustrate individuals' choices.

For example, Verizon may have the worst opt-out implementation that EPIC has ever encountered. In order to opt-out of CPNI sharing from Verizon, one must first notice the privacy notice that appears on the last page of customers' statements. The policy never mentions the word "privacy," and instead is titled "Customer Proprietary Network Information - Special Notice." Additionally, the opt-out policy never specifies that "Customer Proprietary Network Information" refers to calling records—a detailed list of every call an individual makes. This notice is vague and does not adequately inform consumers of the nature of the information collected or the significance of failing to opt-out.

Furthermore, Verizon customers who have attempted to opt-out have encountered a cumbersome and confusing process. Individuals must provide their phone number, their account number, the name on the account, their address, and speak the name of the "authorized" person to make decisions on the account. This process places an unreasonable burden on consumers who simply wish to protect their privacy. Further, the script used by Verizon to guide consumers through the opt-out process employs language that discourages individuals from exercising their rights. For instance, when a consumer chooses to opt-out, the script responds, "You are requesting to establish a restriction on your account"--a characterization that misleads customers about the ramifications of their decision.

The case of *Ting v. AT&T* is also illustrative of this phenomenon. As a response to detariffing, AT&T developed a new standard customer contract.[33] In that case, it was discovered that AT&T actually performed research to ensure that individuals would not read an important consumer notice or take action. AT&T's research showed that reliance on opt-out was sure to result in consumer inaction. The company's market research produced the following recommendation for notices to consumers:

> "In the letter it should be made clear that this agreement is being sent for informational purposes only. The fact that no action is required on the part of the customer needs to be made. A strong link establishing that this information is not a "call to action" on the part of the customer should be clearly stated in the letter...Customers should understand that the mailing is being sent to comply with a federal mandate and does not imply any change in their relationship with AT&T."

[32] *See supra* section II.
[33] *Ting v. AT&T*, 182 F. Supp. 2d 902 (2002).

Because communications providers have a demonstrated history of frustrating consumer notice and choice, we think that opt-in is the appropriate solution for addressing commercial mobile services. There should be no exemption for providers of commercial mobile services.

Respectfully submitted,

Chris Jay Hoofnagle
Associate Director
Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
202.483.1140